Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

KENTUCKY CABINET
FOR HEALTH AND FAMILY SERVICES

070.206 CHFS Remote User Support Policy

Version 2.3
October 25, 2018

Revision History

Date	Version	Description	Author
9/1/2002	1.0	Effective Date	CHFS OATS Policy Charter Team
10/25/2018	2.3	Review Date	CHFS OATS Policy Charter Team
10/25/2018	2.3	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	10/25/2018	Bernard Decker	
CHFS Chief Information Security Officer (or designee)	10/25/2018	Dennis E. Leber	

Table of Contents

1 Policy Definitions

- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Enterprise Identity Management (EIM):** Identity management solution used to provide internal users with network service entitlements.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual’s tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Local Area Network (LAN):** A computer network that links devices within a building or group of adjacent buildings, generally having a radius of less than half a mile.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual’s identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual’s personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother’s maiden name, etc.).
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver’s license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

- **Virtual Private Network (VPN):** A network that is constructed using public wires (i.e. internet) to connect to a private network (i.e. internal network).
- **Wide Area Network (WAN):** A computer network in which the computers connected may be far apart, generally having a radius of half a mile or more.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through an a CHFS Remote User Support Policy. This document establishes the agency's CHFS Remote User Support Policy, which reduces the overall risk(s), and provides guidelines for security best practices regarding remote user support.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 General

Commonwealth Office of Technology (COT) staff has limited ability to support users of CHFS network resources that connect from remote sites that are not under the control of COT Field Services staff. This includes users from contract agencies/companies as well as users connecting from home or while traveling.

Remote Users will be responsible for a logical progression of troubleshooting.

- Contact their Local Area Network (LAN) technician to determine if their LAN and Wide Area Network (WAN) connection is properly configured and operating appropriately. For home users this would be a combination of their local expert and their Internet Service Provider.
- Contact COT via the Commonwealth Service Desk at CommonwealthServiceDesk@ky.gov, to ensure the remote connection hosts are operational. This includes dial up accounts and Virtual Private Networks' (VPN) hosts.
- CHFS technical staff will only be responsible to determine the availability of Cabinet resources once it is determined that a Kentucky Information Highway (KIH) connection exists.

To reduce CHFS liability, IT staff will not make or suggest configuration changes to remote non-CHFS equipment or service equipment at a personal residence.

CHFS staff is subject to follow all guidelines and requirements as outlined in Enterprise IT Policy: CIO-076- Firewall and Virtual Private Network Administration Policy as well as the Office of Human Resource Management (OHRM) Personnel Handbook Chapter 2.11 Telecommuting for remote user access.

4.2 Virtual Private Network (VPN)

COT staff manage all VPN services that utilize the Commonwealth of Kentucky's infrastructure. Virtual Private Network access must be approved and submitted to COT through the Kentucky Online Gateway (KOG) Enterprise Identity Management (EIM) solution by the CHFS division designated personnel. Proper billing information, user information, and approval from authorized agency contact must be obtained and retained when requesting VPN access. CHFS users must follow the CHFS OATS Virtual Private Network (VPN) Procedure when requesting, accessing, removing, or taking any action to a user's VPN account.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

For any staff located within the Department for Behavioral Health, Development, and Intellectual Disabilities (BHDID) who are not on boarded or utilizing KOG, the COT F181EZ Form shall be used to request any action (create, modify, or delete) related to CHFS domain accounts/access. Once forms are competed and approved, they must be submitted to CHFSServiceRequests@ky.gov for completion. Please refer to the COT Forms Page for instructions and more detailed information.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS Intranet: Quotes for IT Purchases and VPN Requests
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: CHFS Virtual Private Network Procedure
- Enterprise IT Form: F181EZ- Staff Service Request, EZ Version, Form
- Enterprise IT Form Instructions: F181i- Staff Services Request Form Instructions
- Enterprise IT Form: F181- Staff Service Request Form (and COT Entrance/Exit Form)
- Enterprise IT Form: F085- Security Exemption Request Form
- Enterprise IT Policy: CIO-076- Firewall and Virtual Private Network Administration Policy
- Internal Revenue Services (IRS) Publications 1075
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Office of Human Resource Management (OHRM) Personnel Handbook Chapter 2.11 Telecommuting
- Social Security Administration (SSA) Security Information